REMARKS

In this Response, Applicants present the following remarks to expedite prosecution and do not acquiesce to any of the Examiner's rejections. Applicants' silence with regard to the Examiner's rejections of dependent claims constitutes a recognition by the Applicants that the rejections are moot based on the Remarks relative to the independent claim from which the dependent claims depend. Applicants reserve the option to further prosecute the same or similar claims in the present or a subsequent application. Claims 1, 4-10, 12, 13, and 15-37 are pending in the present application.

Claim Rejections

35 U.S.C. § 102(b)

The Examiner rejected claims 31-34 under 35 U.S.C. § 102(b) as being anticipated by Ganesan (U.S. Patent Ser. No. 5,748,735), and rejected claims 35-37 under 35 U.S.C. § 102(b) as being anticipated by Linehan et al. (U.S. Patent Ser. No. 5,495,533).

35 U.S.C. § 103(a)

Under 35 U.S.C. § 103(a), the Examiner rejected claims 1, 4-7, 13 and 15-19 as being unpatentable over Ganesan in view of Linehan et al.; claims 8-11 as being unpatentable over Ganesan in view of Linehan et al. and further in view of "Handbook of Applied Cryptography" by Menezes et al.; claim 12 as being unpatentable over Ganesan in view of Linehan et al., in further view of "Handbook of Applied Cryptography" by Menezes et al. and in further view of Carter (U.S. Patent Ser. No. 5,787,175); claim 20 as being unpatentable over Eldridge (U.S. Patent Ser. No. 5,787,169) in view of Linehan et al.; and claims 21-30 as being unpatentable over Eldridge in view Ganesan.

Applicants traverse the rejections under 35 U.S.C. §§ 102(b) and 103(a) in light of the following remarks.

Claims 1, 4-10, and 12

As noted in Applicants previous response, independent claim 1 describes a method by which an entity can store information on an otherwise non-secure server (e.g., a file server) so that only authorized users (e.g., a client) can access it. In accordance with claim 1, a file server stores information encrypted with a first encryption key and uses an access-control list to control access to the encrypted information. The access-control list includes an entry having (a) an identifier for a client that is authorized to at least read the information and (b) a first decryption key that is usable to decrypt the encrypted information and that is encrypted with a second encryption key. The second encryption key is associated with a second decryption key that is accessible to the client and that is usable to decrypt the encrypted first decryption key. In response to a request from the client, the file server transmits the encrypted information and the entry (i.e., the client identifier and the encrypted first decryption key) to the client.

Ganesan teaches data transmission and data storage scenarios. In contrast to independent claim 1 and as recognized by the Examiner (par. 11, page 4 of the Office Action), Ganesan does not teach or suggest transmitting, in response to a request from a client, (i) information that is encrypted with a first encryption key and (ii) a first decryption key that is usable to decrypt the encrypted information and that is itself encrypted with a second encryption key, in which the second encryption key is associated with a second decryption key that is accessible to the client and that is usable to decrypt the encrypted first encryption key.

Linehan et al. teach a networked processing system in which limited access to secure files on a secure workstation is granted to a protected class of users. As described by Linehan et al. (col. 5, lines 6-16), the key client of the creating user uses a key to encrypt a data file to form an encrypted data file which is stored in the encrypted data file memory. The key client of an accessing user sends a ticket validating the user as permitted to operate on the computing system and said data file identification data to a key server. The key server checks the ticket to verify that the accessing user is permitted to access the data file and the key server sends the key corresponding to the data file to the key client of the accessing user. The key client of the accessing user uses the key to decrypt the encrypted data file.

In referencing Linehan et al., the Examiner references the above and contends that the key that the key server sends to the key client of the accessing user is the second decryption key (par. 11, page 5 of the Office Action). However, it is clear from the description of the above method that Linehan et al. do not teach or suggest the use of second encryption/decryption keys to encrypt/decrypt the first key. Linehan et al. specifically recite that "the key server sends the key corresponding to the data file to the key client of the accessing user" (col. 5, lines 13-14).

In an enhanced method, Linehan et al. describe using control keys to encrypt the file encryption key (e.g., col. 8, lines 58-59). However, the "[c]ontrol keys are generated by and kept entirely within the Personal Key Server" (col. 9, lines 11-12) and "known only to the Personal Key Server" (col. 9, line 36). In fact, Linehan et al. describe that the Personal Key Server decrypts the file encryption key and sends the decrypted key back to the Personal Key Client for use in decrypting the data file (col. 9, lines 58). Thus, Linehan et al. do not teach or suggest that the control key (or second key) is accessible to the client, as recited in Applicants' claim 1.

As the Examiner knows, establishing a *prima facie* case of obviousness requires, in part, a teaching of all the claimed limitations. Since neither Ganesan (as acknowledged by the Examiner) nor Linehan et al. teach or suggest a *second decryption key that is usable to decrypt an encrypted first decryption key and that is accessible to a client*, as recited in Applicants' claim 1, it follows that claim 1 is patentable over Ganesan and Linehan et al. Claims 4-10 and 12 depend from claim 1 and are allowable at least by dependency. Reconsideration of the rejection and allowance of claims 1, 4-10 and 12 are respectfully requested.

Claims 13 and 15-19

Independent claim 13 recites a method for securely storing information on a file server and distributing the stored information and including, at least in part, encrypting a first decryption key with a second encryption key for each of a plurality of clients authorized to at least read the information, wherein each respective one of the second encryption keys has a corresponding second decryption key that is usable to decrypt the respective encrypted first decryption key and that is retained by the respective one of the plurality of clients.

With respect to claim 13, the Examiner contends that Ganesan discloses second decryption keys that are usable to decrypt respective encrypted first decryption keys and that are retained by respective clients (col. 6, lines 49-52). However, as noted with respect to claim 1, the Examiner indicated that Ganesan fails to show a second encryption key for encrypting a first decryption key, the second encryption key associated with a second decryption key that is usable to decrypt the encrypted first decryption key and that is accessible to the client (par. 11, page 4 of the Office Action). Applicants agree with the Examiner's characterization of Ganesan with respect to claim 1 and disagree with the Examiner's assertion that Ganesan shows second decryption keys retained by the clients and used to decrypt the encrypted first decryption keys.

As referenced by the Examiner, Ganesan discloses that the file server obtains the symmetric crypto key by applying the first private key portion of the file server's crypto key to decrypt the retrieved encrypted key message (col. 6, lines 49-52). Ganesan does not teach that the user retains the first private key portion of the file server's crypto key. In fact, Ganesan discloses that each file server has a crypto key assigned to it, with a first private key portion known only to that file server (col. 9, lines 40-45). As disclosed by Ganesan, the security server encrypts the crypto key with a second portion of the file server's private key and the file server obtains the symmetric crypto key by applying the first private key portion of the file server's crypto key to decrypt the encrypted key message (col. 10, line 44-58). Thus, Ganesan does not teach or suggest that a *second decryption key that is usable to decrypt the respective encrypted first decryption key is retained by the respective client*, as recited in claim 13. As further shown in the above remarks with respect to claim 1, Linehan et al. also do not teach or suggest a second decryption key is retained by (accessible to) the client.

In addition, the Examiner has recognized that Ganesan fails to show storing the encrypted information on the file server and storing the encrypted first decryption keys on the file server as a plurality of entries within an access control list, with each entry associated with one of the clients. Applicants agree and further note that the Examiner has not asserted that Linehan et al. shows such a teaching. Rather, the Examiner asserts (par. 16, page 7 of the Office Action) that Linehan et al. teach that if the accessing user is permitted to access the data file, the key server sends the first decryption key corresponding to the data file to the key client of the user and the key client uses the key to decrypt the data file (col. 5, line 13-16). Thus, in the Examiner's reference to Linehan et al., it is the key server that maintains the first decryption keys as entries in an access list and the file server that stores the encrypted information. As noted in the above remarks with respect to claim 1, Linehan et al. disclose that control keys are generated by and kept entirely within the key server (col. 9, lines 11-12) and are known only to the key server (col. 9, line 36).

Based on the foregoing, Ganesan and Linehan et al, alone or in combination, do not teach all of the limitations of claim 13. Thus, it follows that claim 13 is patentable over Ganesan and Linehan et al. Claims 15-19 depend from claim 13 and are allowable at least by dependency. Reconsideration of the rejection and allowance of independent claim 13 and claims 15-19 are respectfully requested.

Claim 20

Claim 20 recites a method for storing information securely on a file server for access by members of a group, including, at least in part, forwarding to one of the members, in response to a request received at the file server from the member, the information encrypted with a first key and a first decryption key encrypted with a group encryption key. Applicants agree with the Examiner (par. 28, page 11 of the Office Action) that Eldridge fails to show the above limitation. However, Applicants disagree with the Examiner's assertion that Linehan et al. teach forwarding to a member of the group the encrypted information and the first decryption key encrypted with the group key.

As Applicants have shown in the above remarks with respect to claim 1, Linehan et al. describe using control keys to encrypt the file encryption key, where the control keys are generated by and kept entirely within and known only to a Personal Key Server. The Personal Key Server decrypts the file encryption key and sends the decrypted key back to the Personal Key Client for use in decrypting the data file (col. 9, lines 11-58). Thus, Linehan et al. do not teach or suggest forwarding a first decryption key encrypted with a group key to a member of a group, as recited in Applicants' claim 1. Since neither Eldridge (as acknowledged by the Examiner) nor Linehan et al. teach or suggest such a limitation, it follows that claim 20 is patentable over Eldridge and Linehan et al. Reconsideration of the rejection and allowance of claim 20 are respectfully requested.

Claims 21-30

Claim 21 recites a method for accessing information securely stored on a file server for access by members of a group, including, at least in part, forwarding to one of the members, in response to a request received at the file server from the member, the information encrypted with a first key and a first decryption key encrypted with a group encryption key. Applicants agree with the Examiner (par. 30, page 12 of the Office Action) that Eldridge fails to show the above limitation. However, Applicants disagree with the Examiner's assertion that Ganesan teaches forwarding to a member of the group the encrypted information and the first decryption key encrypted with the group key. Ganesan specifically states that the file server obtains the crypto key by applying a first private key portion to the file server's crypt key to decrypt the encrypted message, obtains the requested data by applying the crypto key to decrypt the encrypted file, and directs the data to the requesting user (col. 6, lines 49-55). Thus, in Ganesan, neither the encrypted information nor the encrypted first decryption key are forwarded to a group member. Since neither Eldridge (as acknowledged by the Examiner) nor Ganesan teach or suggest all of the limitations of claim 21, it follows that claim 21 is patentable over Eldridge and Ganesan. Claims 22-30 depend from claim 21 and are allowable at least by dependency. Reconsideration of the rejection and allowance of independent claims 21-30 are respectfully requested.

Claims 31-37

Claim 31 recites a method for accessing information stored securely on a file server, including receiving the information from the file server encrypted with a first encryption key having an associated first decryption key that is usable to decrypt the encrypted information and an access control list entry associated with a client authorized to read the information. The entry includes the first decryption key encrypted with a second encryption key having an associated second decryption key that is usable to decrypt the encrypted first decryption key and that is accessible to said client. The Examiner contends that Ganesan anticipates claim 31. Applicants disagree. As provided in the above remarks with respect to claims 1 and 13, Ganesan does not teach a second decryption key usable to decrypt an encrypted first decryption key and that is accessible to a client. Applicants also refer the Examiner to the Examiner's statement that Ganesan "fails to show wherein said second encryption key is associated with a second decryption key that is usable to decrypt said encrypted first decryption key and that is accessible to said client" (par. 11, page 4 of the Office Action). Based on the Examiner's statement and Applicants' related remarks above, Ganesan does not teach all of the limitations of claim 31. Thus, it follows that claim 31 is not anticipated by Ganesan. Claims 32-34 depend from claim 31 and are allowable at least by dependency. Reconsideration of the rejection and allowance of independent claim 31 and claims 32-34 are respectfully requested.

Similarly, claim 35-37 recite respective computer program products, computer data signals and apparatus having limitations corresponding to claim 1, at the least. For the reasons set forth above with respect to at least claim 1, Linehan et al. do not anticipate any of claims 35-37. Reconsideration of the rejection and allowance of independent claims 35-37 are respectfully requested.

CONCLUSION

On the basis of the foregoing Remarks, this application is in condition for allowance. Accordingly, Applicants request allowance.

Applicants invite the Examiner to contact the Applicants' Attorney should questions arise concerning this Response.

Respectfully submitted,

Robert W. Gauthier, Reg. No. 35,153
Attorney for Applicants
Tel. No. (617) 832-1175
Fax. No. (617) 832-7000

Date: October 14, 2004
Customer No: 25181
Patent Group
Foley Hoag, LLP
155 Seaport Blvd.
Boston, MA 02210-2600